

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is either anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 542-7800 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Specification amendments

Various amendments have been made to the specification to correct minor inadvertent grammatical and spelling errors.

Status of claims

Claims 1-18 have now been canceled and replaced with new claims 21-31. Claims 19 and 20 have previously been canceled.

The new claims recite the present invention with increased precision and clarity than did the prior claims, and

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

also conform to the dictates of proper US claim practice.
Further, none of the new claims contains a "whereby clause".

Rejections

A. Rejection under 35 USC § 102

The Examiner has rejected prior claims 1 and 2 under the provisions of 35 USC § 102(b) as being anticipated by the teachings of the '633 Lorsch patent (United States patent 5,903,633 issued to R. H. Lorsch on May 11, 1999). Inasmuch as both of these claims have been canceled, this rejection is now moot. Nevertheless, since prior claims 1 and 2 have been replaced by new corresponding claims 21 and 22, then, to expedite prosecution, this rejection will discussed in the context of these new claims and principally with respect to new independent claim 21 (from which claim 22 directly depends). In that context, this rejection is respectfully traversed.

The Examiner takes the position that all the features of prior claim 1, as he interprets that claim, is identically disclosed in the '633 Lorsch patent. In that regard, the Examiner specifically points, in that patent, to the abstract and Figure 2 and specifically, within that figure to, blocks 240, 250, 260 and 270 thereof. As the Examiner will soon appreciate, his position is incorrect with respect to claim 21.

The '633 Lorsch patent teaches apparatus and an associated method for activating a prepaid phone (calling) card and for billing. As indicated, the card has a magnetic strip

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

which stores prepaid phone card information and which, in turn, is read by a point of sale (POS) terminal. To activate the card, subsequent to its sale or transfer to its ultimate user, the card is read by the terminal which communicates with a central computer. The computer compares information stored on the card with information stored in a central database to verify that the card is legitimately being sold or transferred, and, as a result, either authorizes the terminal to activate the card or instructs the terminal to display a message that activation has been denied. Once the card is activated, either the central computer or a separate invoicing computer then prepares an invoice or automatically debits a client's account. This is described, as the Examiner correctly notes, in the abstract of this patent and shown in blocks 240-290 in FIG. 2; and also in col. 3, line 18 et seq, and col. 6, line 26 et seq; and, in conjunction with FIG. 2, col. 7, line 10 through col. 8, line 33.

As described in col. 3, line 11 et seq, the information stored in the magnetic strip specifies: through a stored control code, the phone card itself and the retailer to whom the card was shipped; a PIN of the card; and an 800 gateway number to which the PIN is pointed. This information is processed by the central computer and compared to corresponding information previously stored, under the same PIN, in the central database. During activation, the terminal also transmits data reflective of its own location to the central computer. The processing includes determining whether the location of the POS terminal matches that retrieved through accessing previously stored information using the PIN of the

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

card, thus assessing whether the terminal, by virtue of its physical location, is authorized to authenticate the card. Authentication also alerts the service provider, here being the company that issued the calling card, that the card has passed from a client to an ultimate end user of the card. As a result, the client (e.g., a retailer), who may have paid only a nominal fee for the card, is then billed for a remaining portion of the charge for the card or has its account automatically debited for that charge. See, e.g., col. 3, line 6 et seq.

The present invention is also directed to activating a card, here being a chipcard and including, e.g., a scratch card, used to obtain services through a communications network from a service provider. However, the presently inventive methodology, while also relying on supplying information to a central computer, illustratively a server associated with a service provider, performs activation quite differently than that disclosed in '633 Lorsch patent.

As described in page 1, line 14 et seq of the present specification (references being to the Applicants' counterpart PCT application of which the present application is a US counterpart application), a common type of conventional prepaid phone cards is a "scratch card". By physically scratching away a protective layer on a portion of the surface of the card, such as with a fingernail or a coin edge, a code becomes visible to its user which uniquely identifies the card. To use the scratch card and consume a calling balance which the card represents, the user must first dial an access number of an associated service provider and then enter the code for the card. Once

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

that occurs, the user then enters the number to be called. This process, which relies on entering long series of numbers, is rather cumbersome and thus generally disfavored by users.

Advantageously, the present invention eliminates any need for a user to physically "scratch" the card and then enter a long series of digits for the card code. Card authorization is accomplished electronically through interaction among the card -- specifically circuitry (a "chip") located on the card itself, a terminal into which a user inserts the card for activation, and a remote server, connected to the terminal through appropriate communication infrastructure, for a service provider associated with the card. Through the present invention, the user does not need to remember the card code or retype its numeric/alphanumeric string each time (s)he wants to use the card. Furthermore, the status of the card, i.e., not activated, activated, or exhausted (i.e., having no useable monetary or other balance available for use through the card), is stored on the card and can be displayed to the user through the terminal. Moreover, to prevent or at least reduce the incidence of fraud, an electronic lock is provided on the card. Specifically, the card generates a result for an attempted activation. That result is either, for a proper activation, a correct "challenge" value as supplied to the card by the server, or, for a potentially fraudulent or erroneous activation, a pre-defined error code. The result is communicated back to the server for storage and processing thereat. Moreover, the card circuitry has a predefined limit for the number of times activation can be attempted before it succeeds. Once this number is reached, thus typically indicative of repeated

attempts of fraudulent activation, the server can effectively render the card invalid, thus precluding all further attempts to activate the card. In addition, a user's balance is stored remotely on the server, rather than on the card, thus preventing access to that balance until the card has been properly activated, thus minimizing loss to the legitimate user of the card.

Specifically and in accordance with the Applicants' inventive teachings, a user first obtains card 1, generally being a so-called "chipcard" (as shown in FIG. 1 and discussed in page 4, line 16 et seq). However, to utilize the card to gain services from its associated service provider, the user first needs to activate the card to gain access to a predefined balance, whether monetary or otherwise, which has been given to the card and stored in the server for the service provider and in an account associated with the card. To do so, the user inserts the card into terminal 6 which communicates through infrastructure 7, containing a communications network, with remote server 8 which, in turn, accesses database 10. As indicated in FIG. 2 and described in page 5, line 4 et seq, the card contains internal storage medium 15 (on-board non-volatile memory) which stores card data, that data containing card ID 2, activation code 3 and initial challenge code 4. The card also stores challenge 5 and result 11. Activation code 3, which differs for each card, is similar to a code that could be printed on a conventional chipcard and made visible by "scratching" an overlying surface of that card but is stored in a secure manner within the storage medium.

As described in page 5, line 23 et seq, initial challenge 4 is a code that must be provided, i.e., offered, to the card by the server, via the infrastructure, and from which the card can derive the activation code in order to activate the card. Challenge 5 is a code that indicates a value that has been provided to the card for activating the card and also for obtaining, from the card, its current status (that being not active, active or empty).

In essence and as described in page 6, line 17 et seq, once the user inserts the card into the terminal, the terminal will then access the card data from the storage medium and transmit card ID 2 and challenge code 4 to the terminal. The terminal compares challenge 5 with a predetermined code (referred to as C1, such as the value 111...1) to assess whether the card has not yet been activated (that code having been pre-stored as challenge 5 in the card presumably during its manufacture). If the challenge equals C1, the terminal, sends the card ID to the server, and requests the server to send activation challenge code 9 associated with that specific card ID back to the terminal. To do so, the server appropriately accesses database 10 for the record associated with that card ID. The activation challenge code has a value, which, if identical to the initial challenge stored on the card, enables the card to derive the same activation code, as that which is already stored on the card, from that value. The server sends the activation challenge code to the terminal which, in turn, sends it onward to the card. The card overwrites its stored challenge 5 with the activation challenge code it received from the server. The card then compares the present value of the

stored challenge (which here is now that value just supplied by the server instead of code C1) with initial challenge code 4. If the two match, then the card assigns activation code 3 to result 11. Otherwise, if the two fail to match, the card assigns a predefined error code, referred to as E1, to result 11. Then, the card transmits result 11 to the terminal which, in turn, sends the card ID and that result to the server. In response, the server checks whether the value of that result equals a value of activation code 3 which has been stored in database 10 and associated with that card ID. If a match occurs, then the server activates a balance associated with the card, thus allowing the user to obtain services through the card and from the service provider associated with the server. In doing so, the server, as a threshold matter, checks whether the result does not equal error code E1. Activation only occurs if the result does not equal this error code. Otherwise, the balance is not activated. As indicated in page 8, line 14 et seq, whenever the balance for the card is exhausted, the server assigns a predefined value, referred to as C2, to challenge 5. Should the card be active but its balance not exhausted, then challenge 5 has a value that is equal to neither C1 or C2 but rather to activation challenge code 9. Thus, the value of challenge 5, as stored on the card, reflects the current status of the card: not active, active or empty. If result 11 equals error code E1, then a fraudulent activation attempt has occurred which is reflected in a difference then existing between the values of initial challenge 4 and challenge 5 as they are then both stored on the card.

The basic steps in the Applicants' inventive activation methodology are: inserting the chipcard card into a terminal, and reading card data and transmitting that data from the chipcard, via the terminal, to the server; sending an activation challenge code from the server, via the terminal to the card; determining, in the card, whether the activation challenge code is correct by comparing that code with an initial challenge code stored in the card itself; and if the activation challenge code is correct (i.e., these two match), then sending an activation code stored in the card back to the server in order to activate a balance associated with that card. These steps are shown in graphical form in Figure 1 as follows:

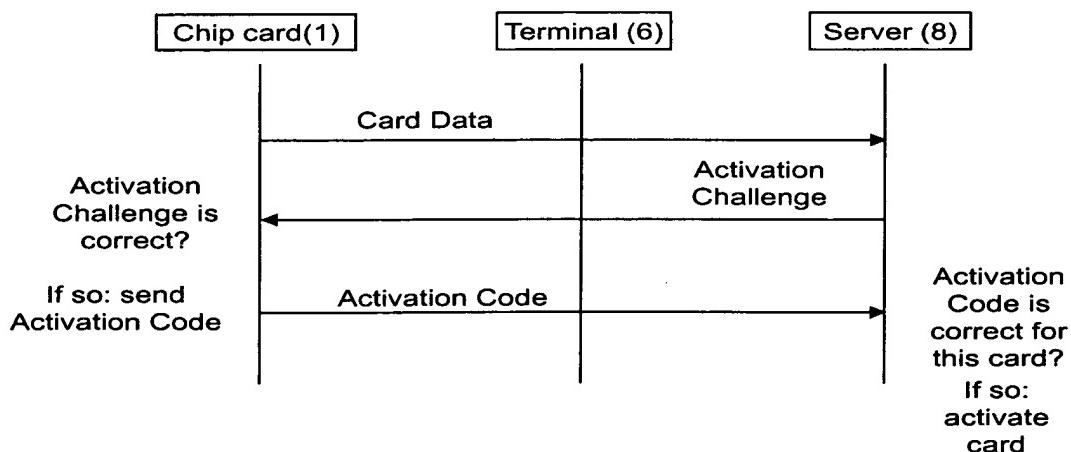


Figure 1 -- APPLICANTS' CHIP CARD PROTOCOL

The '633 Lorsch patent has no disclosures, teachings or even any suggestions regarding the use of an activation

challenge code, let alone in the manner taught by the present Applicants, where that code, upon card activation, is sent by a server, via a network and a terminal, to the card and compared within the card to a stored value for an initial challenge code to determine a match there between and, in the event of such a match, informing the server, through sending a pre-stored activation code, that it can then activate a balance associated with the card.

Independent claim 21 contains suitable recitations directed at distinguishing features of the present invention. Specifically, this claim recites as follows, with its principal distinguishing recitations shown in a bolded typeface:

“A method of activating a chipcard for providing services among a terminal, accessible to a service customer, an infrastructure, comprising a network, and a server connected to the infrastructure and associated with a service provider, **the chipcard having a storage medium containing an activation code and an initial challenge code**, wherein the method comprises the steps of:

inserting the chipcard in the terminal, the terminal being connected, via the infrastructure, to the server;

comparing, within the chipcard, an activation challenge code, received from the server and through the infrastructure and the terminal, with the initial challenge code stored in the storage medium; and

if the activation challenge code equals the initial challenge code, sending the activation code stored in the medium, via the terminal and the infrastructure, to the

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

server for activating a card balance associated with the chipcard." [emphasis added]

Thus, as the Examiner should now appreciate, in the absence of these claimed distinguishing features being disclosed, let alone identically, in the teachings of the '633 Lorsch patent, the Applicants submit that claim 21 is not anticipated by those teachings. Accordingly, this claim is patentable under the provisions of 35 USC § 102(b).

New dependent claim 22 directly depends from new independent claim 21 and recites further distinguishing aspects of the present invention over those recited in the latter claim. Hence, the Applicants submit that claim 22 is also not anticipated by the teachings of the '633 Lorsch patent for the exact same reasons set forth above with respect to claim 21. Consequently, this dependent claim is also patentable under the provisions of 35 USC § 102(b).

Therefore, this rejection should now be withdrawn.

B. Rejection under 35 USC § 103

The Examiner has rejected prior claims 3-18 under the provisions of 35 USC § 103 as being obvious over the teachings in the '633 Lorsch patent taken in view of those in the '580 Molva et al patent (United States patent 5,347,580 issued to R. Molva et al on September 13, 1994). Inasmuch as all these claims have been canceled, this rejection is also now moot. Nevertheless, since these claims have been replaced by new

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

dependent claims 23-31 and all of which depend, either directly or indirectly from new independent claim 21, then, to expedite prosecution, this rejection will be discussed in the context of these new claims and principally with respect to new independent claim 21. In that context, this rejection is respectfully traversed.

The Examiner takes the position that with respect to prior claims 3, 4 and 12, the '633 Lorsch patent does not explicitly teach the concept of a smartcard acting as a scratch card. The Examiner takes Official Notice that the concept of incorporating magnetic strips into cards to, among other reasons, enhance security is well-known. Further, the Examiner concedes that while the '633 Lorsch patent does not teach the concept of a user having to authenticate himself to a smartcard to activate it, doing so is a common feature in the use of smartcards taught by the '580 Molva et al patent (with specific reference being made to col. 2, lines 20-38 in that patent). The Examiner states that having the card provide the capability of authenticating a user inherently requires the card to be able to confirm that it has received a proper code. With these teachings in mind, the Examiner believes it would have been obvious to one of ordinary skill in the art at the time of the Applicants' present invention for a card to "require receiving a proper challenge to activate it for use", thus rendering each of prior claims 3, 4 and 12 obvious presumably over the teachings in the '633 Lorsch patent as modified by those in the '580 Molva et al patent. This conclusion is incorrect with respect to new independent claim 21.

The '580 Molva et al patent describes a technique for authenticating smartcards which relies on using an encrypted time value. This technique considerably differs from the Applicants' inventive methodology.

As described in, e.g., col. 6, line 11 et seq of the '580 Molva et al patent, the smartcard has, among other components, a card identifier, a running value device such as a clock, and an encrypting circuit with a secret key. An overall authentication system includes an authentication server and various distributed workstations connected through the network to the server. The technique taught by that patent involves the basic steps of:

- (a) encrypting, by the card, the running value using a secret card key to yield an encrypted card value;
- (b) receiving, at a workstation, a user name, the card identifier, the card running value, and a user authenticator computed from the user's personal identifier, and the encrypted card value;
- (c) transmitting, through the workstation, to the server, the user name, the card running value, the card identifier and the card value encrypted under the user authenticator;
- (d1) determining, by the server, a potential secret card key from the received card identifier and a potential personal identifier from the received user name;
- (d2) computing, by the server, a potential encryption of the received running value under the potential secret card key and, combining the potential personal identifier and the computed encryption, to obtain a potential user authenticator;

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

- (d3) computing, by the server, computer a potential encryption of the received card running value under the potential user authenticator and comparing this encrypted value to the received encryption value of the card running value under the user's authenticator; and
- (e) if a match of the potential encryption value with the received encryption value occurs, transmitting, by the server, an accept signal back to the workstation.

In contrast, the Applicants' inventive approach does not rely on encrypting a running value, such as time, nor does it compute a user authenticator. Nor does the authentication server used in the present invention need to compute any secret card key.

Further, the '580 Molva et al patent is devoid of any teachings, disclosures or suggestions relating to the inventive concepts of:

- a) the server, upon the start of card authentication, supplying an activation challenge code to the card;
- b) the card, determining whether that code matches an initial challenge code stored within the card itself; and
- c) the card, if a match occurs, issuing an activation code, pre-stored in the card, to the server in order for the server to then activate the card by activating a balance associated with the card.

Since the methodology taught by the Applicants' significantly differs from that taught by the '580 Molva et al patent, then, *a priori*, any hypothetical combination, including

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

that posed by the Examiner, which relies on incorporating the teachings of the '580 Molva et al patent into those of the '633 Lorsch patent would still practice the specific authentication methodology taught by the '580 Molva patent and thus teach in a direction markedly away from the present invention.

As discussed above, independent claim 21 contains suitable recitations directed to principal distinguishing aspects of the present invention.

Thus, the Applicants submit that this claim is not rendered obvious under the provisions of 35 USC § 103 by the teachings in the '663 Lorsch and '580 Molva et al patents regardless of whether those teachings are taken singly or in any combination including those put forth by the Examiner.

Each of dependent claims 23-31 depends, either directly or indirectly, from claim 21 and recites further distinguishing features of the present invention over those recited in claim 21. Consequently, the Applicants submit that each of these dependent claims is also not rendered obvious under the provisions of 35 USC § 103 over the teachings in the '633 Lorsch and the '580 Molva et al patents for the same reasons set forth above with respect to claim 21.

Therefore, this rejection should now be withdrawn as well.

Appl. No. 10/539,084
Amdt. dated May 27, 2009
Reply to Office action of Dec. 12, 2008

Conclusion

Thus, the Applicants submit that none of the claims, presently in the application, is anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103.

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,



May 27, 2009

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 542-7800

MICHAELSON & ASSOCIATES
Counselors at Law
P.O. Box 8489
Red Bank, New Jersey 07701-8489

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **May 27, 2009** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



Signature

30,090

Reg. No.

(PTT207AMDT052209/ca)